ROBBINS GELLER RUDMAN
& DOWD LLP
AELISH M. BAIG (201279)
JACOB G. GELMAN (344819)
Post Montgomery Center
One Montgomery Street, Suite 1800
San Francisco, CA 94104
Telephone: 415/288-4545
415/288-4534 (fax)
aelishb@rgrdlaw.com
jgelman@rgrdlaw.com

Attorneys for Plaintiff and the Class

[Additional counsel appear on signature page.]

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

| | |
|---|---|
| NATHAN COLOMBO, Individually and on Behalf of All Others Similarly Situated,<br><br>Plaintiff,<br><br>vs.<br><br>YOUTUBE, LLC and GOOGLE LLC,<br><br>Defendants. | Case No. 3:22-cv-06987-JD<br><br>CLASS ACTION<br><br>SECOND AMENDED COMPLAINT FOR:<br>(1) Violation of Illinois Biometric Information Privacy Act, 740 ILCS 14/15(b); and<br>(2) Violation of Illinois Biometric Information Privacy Act, 740 ILCS 14/15(a)<br><br>DEMAND FOR JURY TRIAL |

Plaintiff Nathan Colombo ("Colombo") ("Plaintiff" or "Colombo") brings this Second Amended Class Action Complaint against Defendants YouTube, LLC ("YouTube") and Google LLC ("Google") (collectively, "Defendants") to put a stop to Defendants' surreptitious collection, use, and storage of Plaintiff's and the proposed Class' (defined below) sensitive biometric identifiers[1] and biometric information[2] (collectively, "biometrics") without obtaining informed written consent or providing the data retention and destruction policies to consumers. Plaintiff alleges as follows upon personal knowledge as to himself and his own acts and experiences, and, as to all other matters, upon information and belief, including investigation conducted by his attorneys.

## NATURE OF THE ACTION

1. Google is one of the largest corporations in the world. Its business focuses on, among other things, artificial intelligence, Internet search engine technology, online or digital advertising, cloud computing, computer software, quantum computing, e-commerce, and consumer electronics.

2. Google has been referred to as the "most powerful company in the world" and one of the world's most valuable brands due to its market dominance, data collection, and technological advantages in the area of artificial intelligence. It is considered one of the "Big Five" American information technology companies, alongside Amazon.com, Inc., Apple Inc., Meta Platforms, Inc. (f/k/a Facebook), and Microsoft Corporation.

3. Google offers a multitude of products and services beyond its ubiquitous Google Search, many of which hold dominant market positions, including video sharing through YouTube.

4. Google purchased YouTube on November 13, 2006, for $1.65 billion in Google stock. YouTube is now a wholly owned subsidiary of Google.

[1] "'Biometric identifier' means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." 740 ILCS 14/10.

[2] "'Biometric information' means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual." *Id.*

5. Google and YouTube operate the two most visited websites worldwide, google.com and youtube.com.[3]

6. Google.com and youtube.com are also the two most visited websites in the United States.[4]

7. Founded in 2005, YouTube is the largest social media video-sharing platform in the world.

8. YouTube's platform has more than 2.5 billion monthly users who collectively watch more than one billion hours of videos each day.

9. As of May 2019, videos were being uploaded to YouTube at a rate of more than 500 hours of content per minute.

10. YouTube users can use the YouTube platform to, among other things, upload and share videos, either privately or with the general public.

11. Once a user uploads a video on YouTube, the user can use various YouTube features or tools to, among other things, blur out faces within an uploaded video and/or create thumbnail photographs of various points within a particular video.

12. As alleged in more detail below, Defendants' "Face Blur" tool allows a user to "select the faces" in the user's particular video that they would "like to blur," which when applied and saved, will result in those faces appearing blurry and ostensibly unrecognizable to any viewer of the video.

13. In order for a YouTube user to use the "Face Blur" tool, the user must use YouTube Studio, which Defendants claim is "the home for creators[,]" and allows YouTube users to "manage [their] presence, grow [their] channel, interact with [their] audience, and make money all in one place."[5]

---

[3] *Most Visited Websites by Traffic in the world for all categories, July 2022*, SEMRUSH, https://www.semrush.com/website/top/.

[4] *Most Visited Websites by Traffic in United States for all categories, July 2022*, SEMRUSH, https://www.semrush.com/website/top/united-states/all/.

[5] *Navigate YouTube Studio*, GOOGLE, https://support.google.com/ youtube/answer/ 7548152?hl=en (last visited Aug. 29, 2022).

14. Upon information and belief based on the investigation of Plaintiff's counsel, Defendants' "Face Blur" tool captures and stores biometric identifiers or information in the form of scans of the face geometry of individuals appearing in the videos that the tool is used on, including for videos uploaded within the state of Illinois. This captured information is capable of being used to identify the individuals in the videos. However, Defendants do not provide notice or obtain legally mandated consent from the Illinois residents whose biometric identifiers or information is captured, in violation of Illinois' Biometric Information Privacy Act, 740 ILCS 14/1, *et seq.* ("BIPA"). Nor do Defendants post a publicly available retention schedule and guidelines for permanently destroying the biometric identifiers of Plaintiffs and the Class, as mandated by BIPA, or comply with any such guidelines.

15. The uploading, Defendants' capture, and Defendants' use of these biometric identifiers or information of Plaintiff and all Class members all take place in the state of Illinois. Defendants' failure to post a publicly available retention schedule and guidelines for permanently destroying such biometric identifiers, along with their failure to comply with such, also took place in Illinois.

16. In addition, Defendants offer YouTube users an opportunity to choose specific thumbnail pictures culled from an uploaded video. Specifically, YouTube contains a feature that allows video creators to choose thumbnails for their videos that are auto generated by YouTube.

17. To be sure, thumbnails with faces, especially faces with more expression, generate more clicks and views and, as such, Defendants are incentivized to auto-generate thumbnails that contain faces – especially faces that contain more expression.

18. Upon information and belief based on the investigation of Plaintiff's counsel, Defendants' thumbnail feature works by scanning the uploaded video and all faces within the video to identify facial expressions, including for videos uploaded within the state of Illinois. The purpose of this is to attract the most clicks and views for the uploaded videos. In doing so, Defendants capture and store biometric identifiers or information that are capable of being used to identify the individuals in the videos in the form of faceprints without providing notice or obtaining legally mandated consent from the Illinois resident whose biometric identifiers or information is

captured, in violation of BIPA. Nor do Defendants post a publicly available retention schedule and guidelines for permanently destroying the biometric identifiers of Plaintiff and the Class, as mandated by BIPA, or comply with any such guidelines.

19. The uploading, Defendants' capture, and Defendants' use of Plaintiff's and Class members' biometric identifiers or information from Defendants' thumbnail feature all take place in the state of Illinois. Defendants' failure to post a publicly available retention schedule and guidelines for permanently destroying such biometric identifiers, along with their failure to comply with such, also took place in Illinois.

20. Through these practices, Defendants not only disregard their Illinois users' privacy rights, they also violate BIPA, which was specifically designed to protect Illinois consumers from practices like those of Defendants. In particular, Defendants violated (and continue to violate) BIPA because they did not:

(a) properly inform Plaintiff or the Class in writing that their biometric identifiers, which can be used to identify these individuals, were being collected or stored;

(b) properly inform Plaintiff or the Class in writing of the specific purpose and length of time for which their biometric identifiers were being collected, stored, and used;

(c) provide a publicly available retention schedule and guidelines for permanently destroying the collected and stored biometric identifiers of Plaintiff and the Class (or comply with any such guidelines); and

(d) receive a written release from Plaintiff or the Class to collect, capture, or otherwise obtain their biometric identifiers.

21. Accordingly, this Complaint seeks a final judgment: (a) declaring that Defendants' conduct violates BIPA; (b) requiring Defendants to cease the unlawful activities discussed herein; and (c) awarding statutory damages to Plaintiff and the Class.

## PARTIES

22. Plaintiff Nathan Colombo is a natural person and resident and citizen of the State of Illinois residing in Carbondale, Illinois in Jackson County. Plaintiff has been a customer of Google and a registered and active user of YouTube since at least March 2020. Within the applicable statute of limitations period, and from within the state of Illinois, Colombo uploaded multiple videos to YouTube and used Defendants' "Face Blur" tool or thumbnail creator containing at least one representation of his face, which Defendants captured in the state of Illinois, scanned for face geometry, and stored, without providing Colombo any notice or receiving a written release in violation of BIPA.

23. Defendant YouTube, LLC is a limited liability company organized and existing under the laws of the State of Delaware, and is headquartered in San Bruno, California. YouTube is a wholly owned subsidiary of Google.

24. Defendant Google LLC is a limited liability company organized and existing under the laws of the State of Delaware, and is headquartered in Mountain View, California. Google is an online advertising technology company providing internet-related products, including YouTube. Google is owned by Alphabet Inc., a publicly traded company incorporated and existing under the laws of the State of Delaware and headquartered in Mountain View, California.

## JURISDICTION AND VENUE

25. This Court has jurisdiction pursuant to 28 U.S.C. §1332(d)(2)(A), because at least one member of the Class is a citizen of a different state than Defendants, there are more than 100 members of the Class, and the aggregate amount in controversy exceeds $5,000,000, exclusive of interest and costs.

26. This Court has personal jurisdiction over Defendants because Defendants stipulated to such, *see* ECF 25; Defendants are citizens of California; Defendants registered to, and do in fact, conduct substantial business throughout California, including in this District; and Defendants maintain their respective headquarters in California, which are their principal places of business.

27. Venue is proper in this Court pursuant to 28 U.S.C. §1391 because Defendants stipulated to such pursuant to 28 U.S.C. §1404, *see* ECF 25, and because Defendants:

(a) are authorized to conduct business in this District and have intentionally availed themselves of the laws and markets within this District;

(b) conduct substantial business in this District; and

(c) are subject to personal jurisdiction in this District.

## FACTUAL BACKGROUND

### I. Google

28. Google was launched in 1998 as a general online search engine. Founded by Larry Page and Sergey Brin, the corporation got its start by serving users web results in response to online queries. Google's key innovation was its PageRank algorithm, which ranked the relevance of a webpage by assessing how many other webpages linked to it. In contrast with the technology used by rival search engines, PageRank enabled Google to improve the quality of its search results even as the web rapidly grew. While Google had entered a crowded field, by 2000, it had become the world's largest search engine.

29. Today, Google is ubiquitous across the digital world, serving as the infrastructure for core products and services online. It has grown and maintained its search engine dominance, such that "Googling" something is now synonymous with online search itself. The company is now also the largest provider of digital advertising, a leading web browser, a dominant mobile operating system, and a major provider of digital mapping, email, video hosting, cloud computing, and voice assistant services, alongside dozens of other offerings. Nine of Google's products – Android, Chrome, Gmail, Google Search, Google Drive, Google Maps, Google Photos, Google Play Store, and YouTube – have more than a billion users each.

30. Google established its position through acquisition, buying up successful technologies that other businesses had developed. In a span of 20 years, Google purchased well over 200 companies.

31. Google is now one of the world's largest corporations. For 2021, Google reported total consolidated revenues of over $257 billion – up 41% from 2020 – and more than $76 billion in net income.[6]

**II. YouTube**

32. YouTube was founded in 2005. It was the brainchild of Chad Hurley, Steve Chen, and Jawed Karim, who were all former employees of PayPal.

33. According to YouTube's founders, the idea was born at a dinner party in San Francisco, about a year earlier, in 2004. The trio was frustrated by how hard it was, at the time, to find and share video clips online. '"Video, we felt, really wasn't being addressed on the Internet,'" said Chad Hurley in an early interview. '"People were collecting video clips on their cell phones . . . but there was no easy way to share [them]."'[7]

34. By September 2005, YouTube had managed to get its first video with one million views. This was a Nike ad that went viral.

35. Venture capitalists began pouring millions of dollars into YouTube in late 2005.

36. In February 2006, YouTube for the first time added user profile personalization. The personalization of profiles feature was further refined in June 2006.

37. Just a few months later, in October 2006, Google acquired YouTube for $1.65 billion. At the time, Google called YouTube, "the next step in the evolution of the Internet."[8]

38. In December 2009, YouTube's automatic speech recognition service was launched.

39. In July 2012, Google launched YouTube's face-blurring tool, ostensibly to protect the anonymity of protesters and individuals engaging in civil disobedience around the world.[9] According to THE GUARDIAN,

---

[6] Alphabet, Inc. Annual Report on Form 10-K for fiscal year ended Dec. 31, 2021 at 36, https://www.sec.gov/Archives/edgar/data/1652044/000165204422000019/goog-20211231.htm.

[7] Christopher McFadden, *YouTube's History and Its Impact on the Internet*, INTERESTING ENGINEERING (May 20, 2021), https://interestingengineering.com/culture/youtubes-history-and-its-impact-on-the-internet.

[8] *Id*.

[9] Amanda Conway, Face blurring: when footage requires anonymity, YouTube Official Blog (July 18, 2012), https://blog.youtube/news-and-events/face-blurring-when-footage-requires/.

> YouTube users who upload a video to the site are asked whether they want to apply a "Blur All Faces" option which will obscure all identities in the clip. Once faces have been obscured, YouTube creates two versions of the video, one without the blurring and one with. Users can decide whether to publish either or both of the videos. If they choose to delete the unblurred version, it will be removed permanently from Google's servers.[10]

## III. Biometrics and Consumer Privacy

40. "Biometrics" refers to technologies used to identify an individual based on unique physical characteristics. Common biometric identifiers include retina or iris scans, fingerprints, voiceprints, or hand or face geometry scans. One of the most prevalent uses of biometrics is facial recognition technology, which works by scanning an image for human faces, extracting facial feature data, and comparing them against information stored in a "faceprint database." If a database match is found between the extracted facial data and the "biometric identifier" (*i.e.*, details about the face's geometry), a person may be identified.

41. The recent sophistication of facial recognition software has generated many commercial applications of the technology, but has also raised serious privacy concerns about its massive scale, scope, and surreptitiousness.[11] During a 2012 United States Senate hearing, a Senator noted that someone armed with a faceprint can find that person's "name, . . . social networking account, . . . and can find and track [them] in the street, in the stores [they] visit, the Government buildings [they] enter, and the photos [their] friends post online."[12] Faceprints can

---

[10] Josh Halliday, Google introduces face-blurring to protect protesters on YouTube, The Guardian (July 19, 2012), https://www.theguardian.com/technology/2012/jul/19/face-blurring-technology-youtube-protestors#:~:text=Google%20introduces%20face%2Dblurring%20to%20protect%20protesters%20on%20YouTube,This%20article%20is&text=Human%20rights%20activists%20 and%20campaigners,blurring%20technology%20to%20the%20website.

[11] What Facial Recognition Technology Means for Privacy and Civil Liberties: Hearing Before the Subcomm. on Privacy Tech & the Law of the S. Comm. on the Judiciary, 112th Cong. 1 (July 18, 2012) (statement of Jennifer Lynch, Staff Attorney, Electronic Frontier Foundation), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2134497.

[12] *What Facial Recognition Technology Means for Privacy and Civil Liberties: Hearing Before the Subcomm. on Privacy Tech & the Law of the S. Comm. on the Judiciary*, 112th Cong. 1 (July 18, 2012) (statement of Sen. Al Franken, Chairman, Subcomm. on Privacy, Tech. & the Law of the S. Comm. on the Judiciary). https://www.govinfo.gov/content/pkg/CHRG-112shrg86599/pdf/CHRG-112shrg86599.pdf.

be used even to identify protesters from afar and then "target them for selective jailing and prosecution[.]"[13]

42. Unlike other identifiers, such as Social Security or credit card numbers, which can be changed if compromised or stolen, biometric identifiers linked to a specific voice or face cannot. These unique, permanent, and immutable biometric identifiers, once exposed, leave victims with no means to prevent identity theft and unauthorized tracking. Recognizing this, the Federal Trade Commission urged companies using facial recognition technology to ask for consent from consumers ***before*** ever scanning and extracting biometric data from their digital photos.[14] Defendants have ignored this, failed to obtain user consent before launching their wide-spread facial recognition program, and by collecting and using these biometric identifiers in the state of Illinois, violated millions of Illinois residents' legal privacy rights.

## IV. Illinois' Biometric Information Privacy Act

43. BIPA was enacted in 2008. Under BIPA, a company may not "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier[[15]] . . . unless it first:

> (1) informs the subject . . . in writing that a biometric identifier . . . is being collected or stored;
>
> (2) informs the subject . . . in writing of the specific purpose and length of term for which a biometric identifier . . . is being collected, stored, and used; and
>
> (3) receives a written release executed by the subject of the biometric identifier[.]"

740 ILCS 14/15(b).

---

[13] *Id.*

[14] *See Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies*, Federal Trade Commission (Oct. 2012), http://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf.

[15] BIPA's definition of "biometric identifier" expressly includes information collected about the geometry of the face (*i.e.*, facial data obtained through facial recognition technology, like the data collected by Defendants about Plaintiff and the Class). *See* 740 ILCS 14/10.

44. BIPA also regulates how companies must handle Illinois consumers' biometric data. *See, e.g.*, 740 ILCS 14/15(c)-(d). For instance, BIPA prohibits selling, leasing, trading, or otherwise profiting from a person's biometric data, 740 ILCS 14/15(c), and requires that companies develop a publicly available written policy establishing a retention schedule and guidelines for permanently destroying biometric data when the initial purpose for collecting such data has been satisfied or within three years of the individual's last interaction with the company, whichever occurs first, 740 ILCS 14/15(a).

## V. Google Has a History of Violating BIPA

45. In 2016, Google was sued for violating BIPA in connection with its Google Photos product.[16]

46. In general, plaintiffs in *Rivera* alleged that Google violated BIPA in the following manner:

> Google has created, collected and stored, in conjunction with its cloud-based "Google Photos" service, the "face templates" (or "face prints") – highly detailed geometric maps of the face – of millions of users of the Google Photos service and hundreds of thousands of individuals who are not even enrolled in the Google Photos service. Google creates these templates using sophisticated facial recognition technology that extracts and analyzes data from the points and contours of faces that appear in photos taken on Google "Droid" devices and uploaded to the cloud-based Google Photos service. Each face template that Google extracts is unique to a particular individual, in the same way that a fingerprint or voiceprint uniquely identifies one and only one person.[17]

47. Google settled *Rivera* by agreeing to pay $100 million to a class of Illinois residents who alleged that their faceprints were captured by Google.[18]

---

[16] Class Action Complaint, *Rivera v. Google LLC*, No. 1:16-cv-02714 (N.D. Ill. Mar. 1, 2016), ECF 1.

[17] Second Amended Consolidated Complaint at 3, *Rivera v. Google LLC*, No. 1:16-cv-02714 (N.D. Ill. Mar. 7, 2017), ECF 63. Plaintiffs in *Rivera* also sued Google in Cook County, Illinois Circuit Court Chancery Division. *See* Class Action Complaint, *Rivera v. Google LLC*, No. 2019-CH-00990 (Ill. Ch. Ct. Jan. 24, 2019).

[18] *See* Jon Fingas, *Google settles Photos facial recognition lawsuit for $100 million*, ENGADGET (June 6, 2022), https://www.engadget.com/google-photos-bipa-lawsuit-settlement-161237789.html.

48. Importantly, the *Rivera* settlement expressly covers only Google's violation of BIPA arising out of its Google Photos product.[19] Nor could the release in *Rivera* conceivably cover Defendants' ongoing BIPA violations via YouTube, under the long-standing "identical factual predicate" doctrine.[20]

## VI. Defendants Continue to Violate BIPA in Myriad Ways

### YouTube's "Face Blur" Tool

49. As noted, Defendants launched the "Face Blur" tool for YouTube in 2012.

50. Unbeknownst to the average Illinois resident, Defendants' "Face Blur" tool relies on state-of-the-art facial recognition technology to scan videos (including those uploaded within the state of Illinois), locate human faces, and create and store scans of face geometry. The uploading, collection, and use of such scans of face geometry all take place in the state of Illinois, where the Illinois user is located. This information, and face geometry in particular, is capable of being used to identify the individuals whose face geometry is scanned.

51. Figure 1 below shows that the "Face Blur" tool is available as one of five tools on the YouTube "Video Editor" interface.

19 *See* Settlement Agreement at 9, *Rivera v. Google LLC*, No. 2019CH00990 (Ill. Ch. Ct. Apr. 13, 2022) (defining "Released Claims").

20 *See Wal-Mart Stores, Inc. v. Visa U.S.A., Inc.*, 396 F.3d 96, 107 (2d Cir. 2005); *Williams v. Gen. Elec. Cap. Auto Lease, Inc.*, 159 F.3d 266, 273 (7th Cir. 1998).

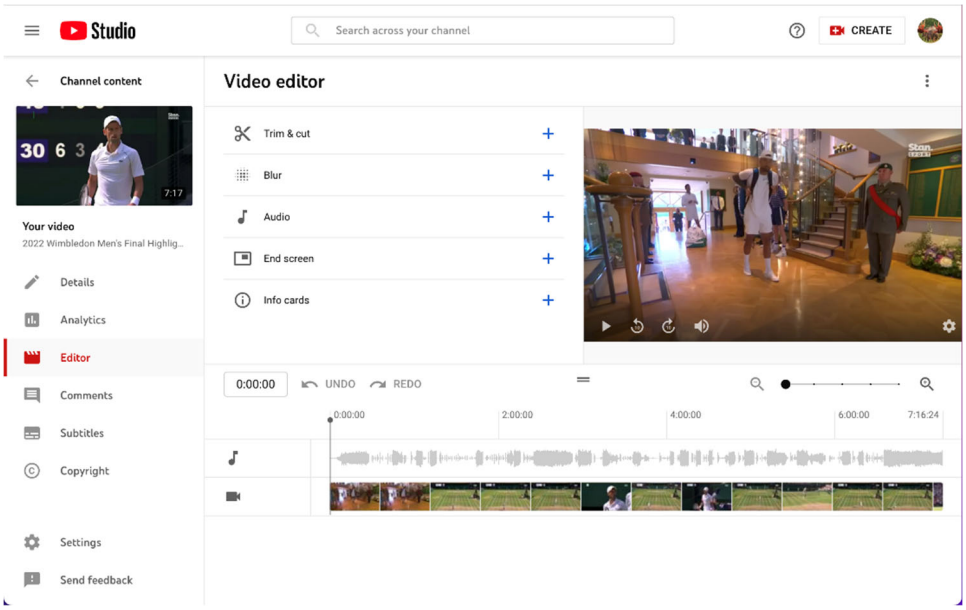


Fig. 1

52. When a YouTube video creator chooses to run the "Face Blur" tool on a video, Defendants scan the entire video to detect all unique faces within the video, as shown in Figure 2 below. This scan generates information that can be used to identify the individuals whose face geometry is scanned.

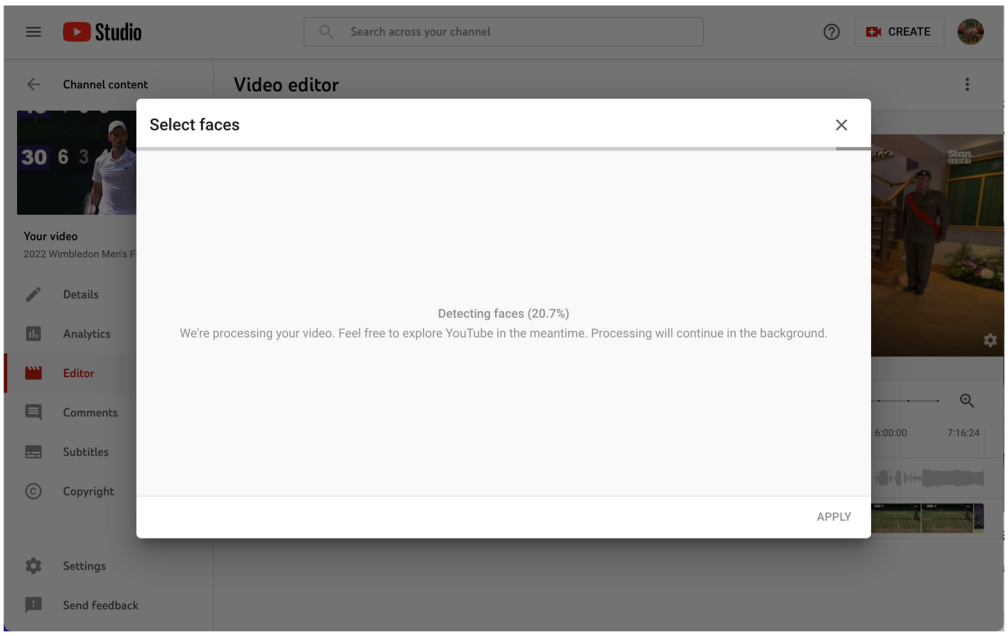


Fig. 2

53. Once Defendants finish scanning the video and generating this identifying information, Defendants display all detected faces within the video and allow the creator to select which faces the creator would like to blur out in the video, as shown in Figure 3 below.

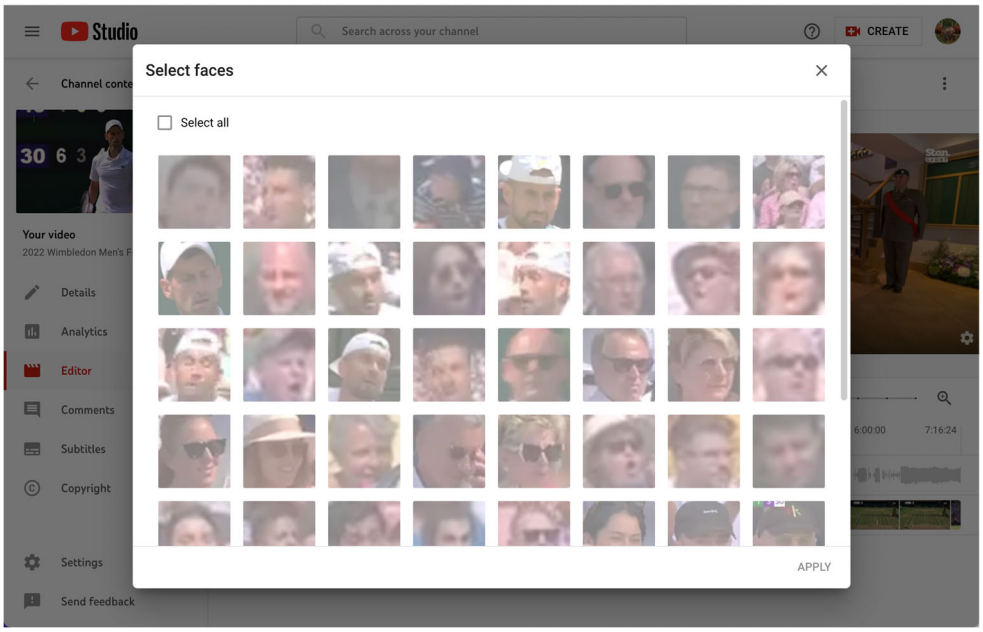


Fig. 3

54. After a creator selects a face from the list of all detected faces and applies the "Face Blur" tool, Defendants blur out the selected face throughout the duration of the YouTube video, as shown in Figure 4 below.

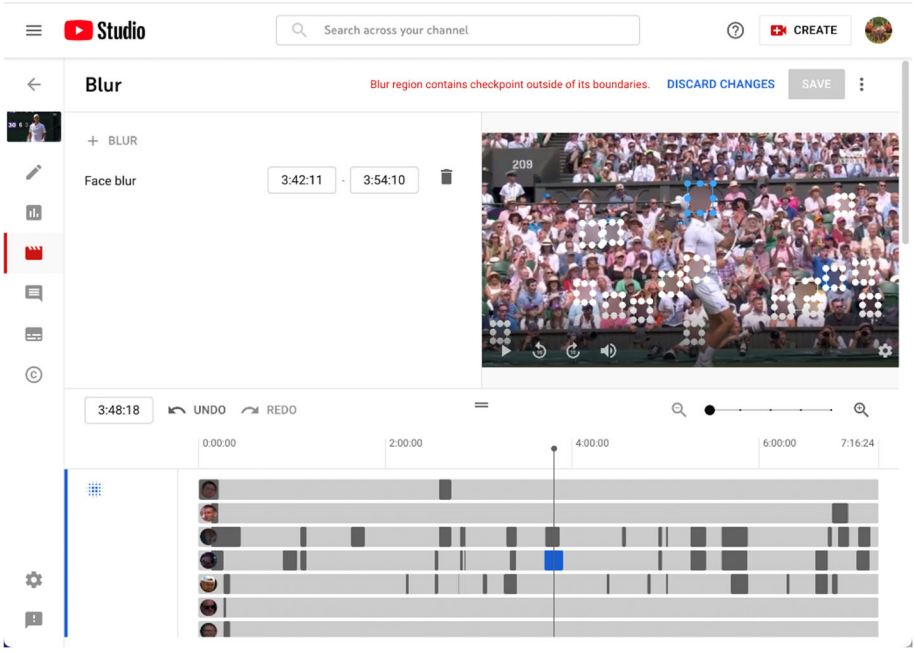


Fig. 4.

55. The underlying computer code depicted in Figure 5 below demonstrates that when a YouTube user employs Defendants' "Face Blur" tool, Defendants capture and store identifying information of the scanned individuals in the form of scans of face geometry from all detected faces, or biometric information and identifiers. This is seen by the unique "faceId" and associated image representation of the faces in the code pictured in Figure 5 below. Defendants use the "faceId" to match with the specific facial geometry captured and stored by Defendants. Then, when users select a "faceId," Defendants blur any matching facial geometry stored on Defendants' servers. In other words, Defendants used the captured biometric information to personally identify the individuals selected as part of the tool's use.

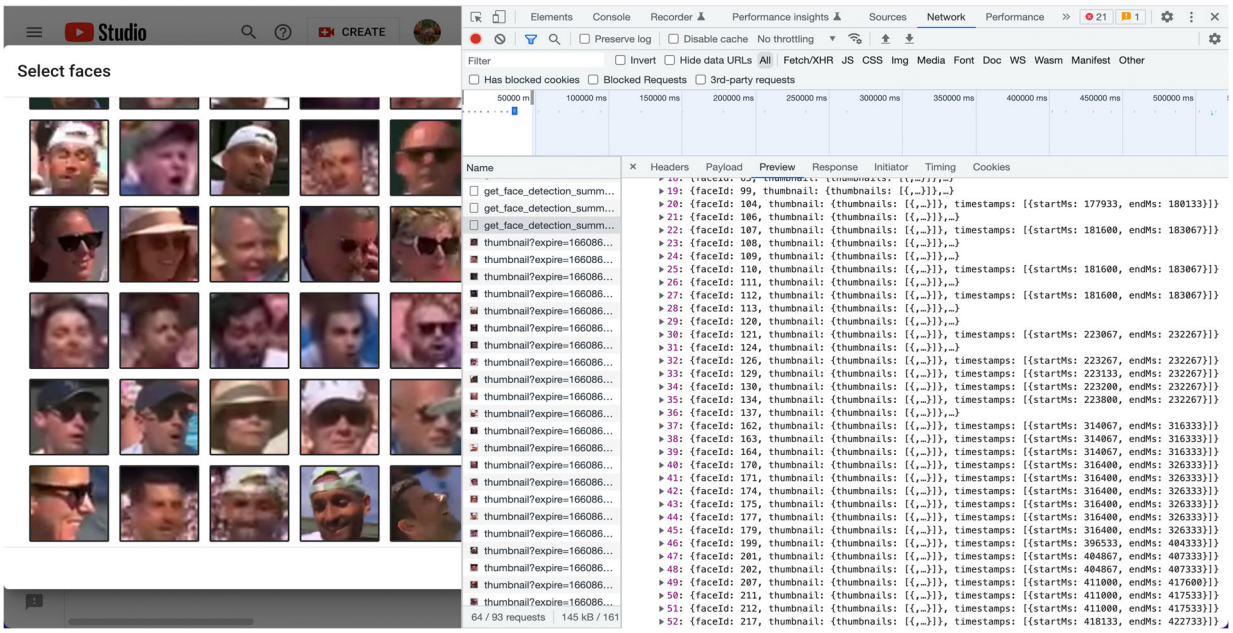


Fig. 5.

56. At first glance, it appears that Defendants are only storing the detected faces for a total of four hours because each detected face comes with an expiry date within a few hours of running the face detection. This is shown in Figure 6 below:

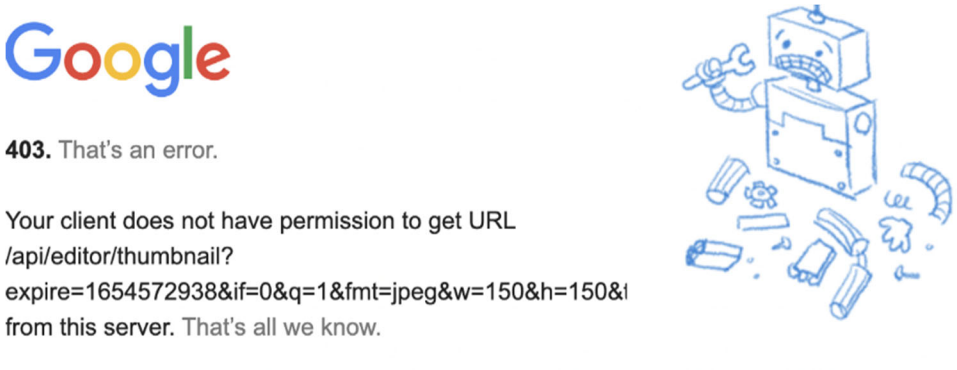


Fig. 6.

57. However, further investigation reveals that Defendants are actually storing the scan of face geometry for a longer period of time, and possibly permanently.

58. This is demonstrated by the fact that, when the "Face Blur" tool is run multiple times on the same video, the previously stored result is provided to the user without actually rerunning the tool again. This is true even when the "Face Blur" tool is run multiple weeks after initially running the "Face Blur" tool – even though Defendants represent to no longer have access to the detected faces after a few hours. *See* Figure 7 below. In other words, the "Face Blur" tool recognizes the individuals appearing in the video as persons who have already been identified and assigned a unique "faceId" through a previous use of the tool.

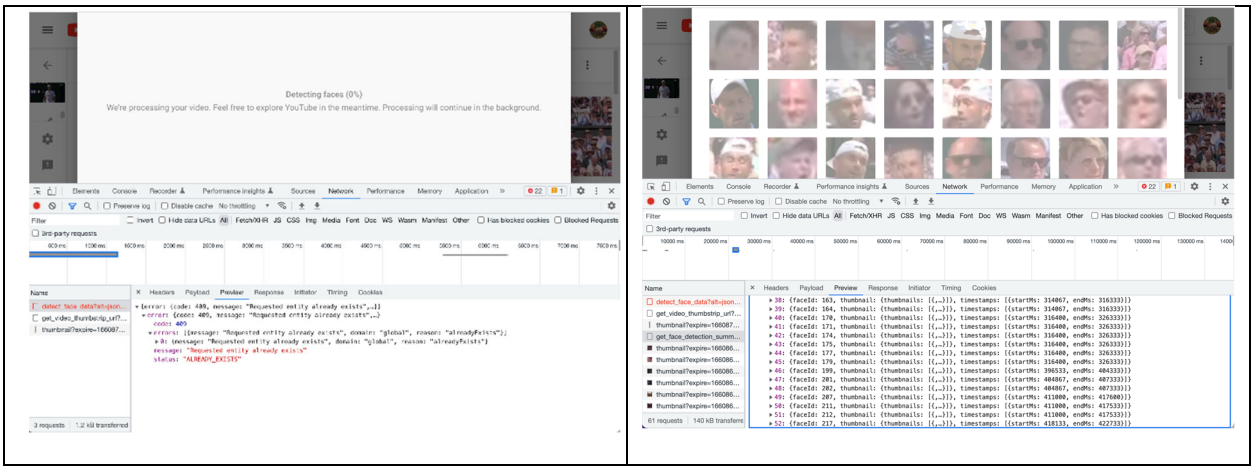


Fig. 7.

59. Consequently, Defendants permanently store scans of face geometry or biometric information so that YouTube users do not need to re-run the "Face Blur" tool.

60. Defendants do not disclose this collection and storage of biometric information or identifiers anywhere, neither in their Terms of Service or elsewhere.

61. Even if Defendants did disclose the collection and storage of biometric information or identifiers to the creator of the video who used the "Face Blur" tool, it would still be a legally insufficient disclosure with respect to the specific individuals whose images were captured and stored from within the video.

62. The uploading, Defendants' capture, and Defendants' use of Plaintiff's and Class members' biometric identifiers, and Defendants' failure to post a publicly available retention schedule and guidelines for permanently destroying such biometric identifiers, along with their failure to comply with such, also took place in Illinois.

63. Accordingly, Defendants have violated and continue to violate the rights of Plaintiff and the Class under BIPA.

**YouTube's Thumbnail Generator**

64. Defendants also include with YouTube a feature that at first auto-generates photographic thumbnails (screenshots from an uploaded video) and allows creators to choose their own thumbnails for their videos.[21]

65. It is common knowledge that thumbnails with faces, especially faces with more expression, generate more clicks and views. As such, Defendants have a huge financial incentive to auto-generate thumbnails that contain faces – especially faces that contain more expression.

66. Upon information and belief, in order to generate optimal thumbnails, Defendants scan all videos uploaded to YouTube, including those uploaded by Plaintiff and the Class within Illinois, for faces at the time the videos are uploaded, and then use this face data to auto-generate thumbnails that contain faces, and especially faces with more expression. Again, the information produced in generating these thumbnails can be used to identify the individuals scanned from the videos.

67. An experiment conducted by Plaintiff's counsel verifies Plaintiff's allegations. Three videos of approximately 60 seconds long were uploaded to YouTube. Each video contained a face within the video for less than two seconds. The remainder of the video contained other content (*e.g.*, cars driving, scenery out of the window, a house tour). In ***each*** of the three videos, Defendants' thumbnail generator, without prompting, auto-generated and applied as the ***main*** thumbnail a face that was only in the video for less than two seconds. A sample illustrating this is in Figure 8 below:

[21] *Add video thumbnails on YouTube*, YOUTUBE, https://support.google.com/youtube/answer/72431?hl=en#zippy=%2Cwhy-are-my-custom-thumbnails-turned-off (last visited Aug. 29, 2022).

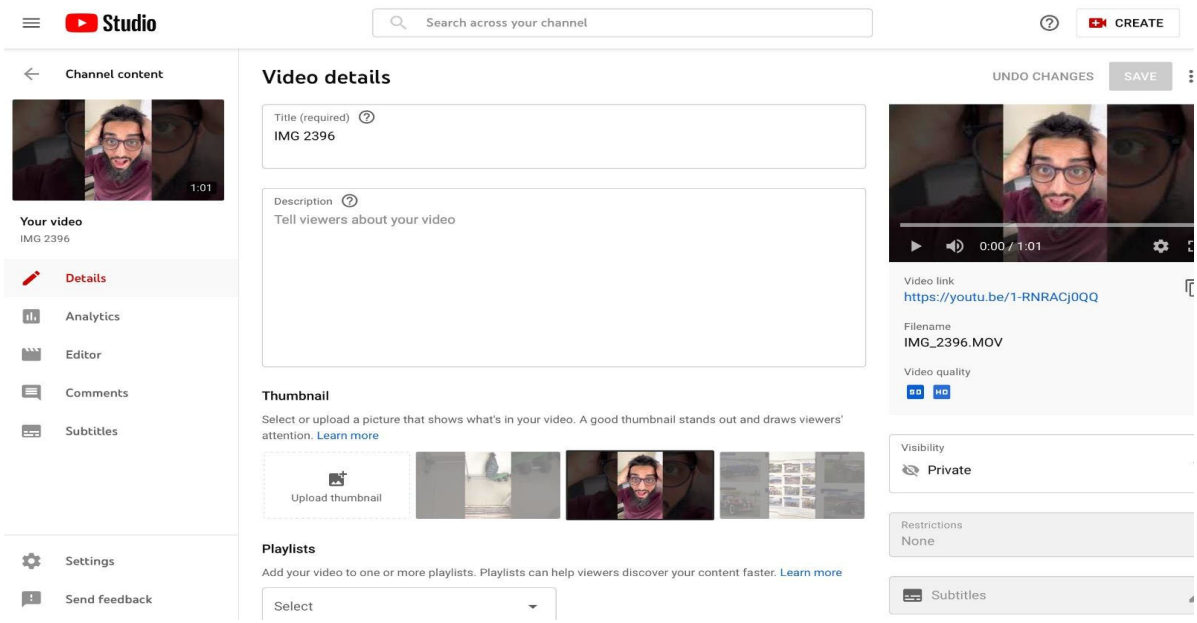


Fig. 8.

68. This indicates that, as part of the thumbnail generator, Defendants have a software program that has been trained to detect faces. This software program would require scans of facial geometry from YouTube videos, including those uploaded within Illinois, as a necessary input in order to train this software. Further, it is likely that the software is continually being optimized by gathering more facial geometry data from YouTube videos.

69. Defendants' own research from 2021 also indicates that it has analyzed millions of videos to detect faces. The research states that it used software "similar to the Google Cloud Face Detection API" to scan and detect faces, follow faces over the course of the video, and label facial expressions in the videos.[22]

[22] *Understanding Contextual Facial Expressions Across the Globe*, GOOGLE AI BLOG (May 24, 2021), https://ai.googleblog.com/2021/05/understanding-contextual-facial.html.

70. However, Defendants' software differs from Google Cloud Face Detection in a critical way. According to the Google Cloud API Documentation, "Specific individual Facial Recognition is not supported" by Google Cloud Face Detection.[23] Defendants' software, on the other hand, distinguishes between individual faces, assigns them unique "faceIds," and allows users to selectively blur some faces while retaining others.

71. Based on the above, it appears that Defendants are scanning each uploaded YouTube video, including those uploaded within Illinois, for faces, and auto-generating thumbnails with expressive facial expressions. During this process, Defendants are scanning, detecting, and collecting facial geometry within each YouTube video, including videos uploaded within Illinois, and then storing the metadata associated with the videos. Defendants store these biometrics for much longer than suggested, maybe indefinitely.

72. The uploading, Defendants' capture, and Defendants' use of Plaintiff's and Class members' biometric identifiers, and Defendants' failure to post a publicly available retention schedule and guidelines for permanently destroying such biometric identifiers, along with their failure to comply with such, also took place in Illinois.

**The Face Geometry and Biometric Identifiers Used in Both Tools**

73. Face geometry analysis is used as part of facial recognition software, like Defendants' "Face Blur" and thumbnail generator tools. This kind of analysis mathematically maps faces and produces unique signatures:

74. Facial recognition software reads the geometry of your face. Key factors include the distance between your eyes and the distance from forehead to chin. The software identifies facial landmarks – one system identifies 68 of them – that are key to distinguishing your face. The result: your facial signature.[24]

[23] Google Cloud, Cloud Vision API, Detect Faces, https://cloud.google.com/vision/docs/detecting-faces (last visited Dec. 12, 2022).

[24] *See* Steve Symanovich, *What is facial recognition? How facial recognition works*, NORTON BLOG (Aug. 20, 2021), https://us.norton.com/blog/iot/how-facial-recognition-software-works.

75. The data generated from these unique facial "landmarks" can be used to uniquely identify the individuals scanned by the facial recognition software:

> Your facial signature — a mathematical formula — [can be] compared to a database of known faces. And consider this: At least 117 million Americans have images of their faces in one or more police databases. According to a May 2018 report, the FBI has had access to 412 million facial images for searches.[25]

76. Unlike a password or security personal identification number, once your biometric identifiers have been collected, there is no un-ringing the bell. Worse, even if the biometric identifiers collected by a company are not immediately exploited, that permanent, personally identifying data could be compromised in a future data breach or later commoditized in advertising.

77. This is why the mere collection and storage of biometric identifiers that ***could*** be used in identifying an individual, under BIPA, requires disclosure and consent. *See* 740 ILCS 14/15(b).

**Defendants Never Require Illinois Users to Acknowledge Their Biometric Data Collection Practices, Never Obtain Their Express Written Consent to Collect the Same, and, Instead, Hide the Fact that They Systematically Collect Illinois Users' Biometrics**

78. Since Defendants' "Face Blur" tool debuted in 2012, and for as long as Defendants' thumbnail creator has been available, Defendants have never disclosed their collection and storage of Plaintiff's and Class members' biometric data, which can be used to identify the individuals scanned from the videos.

79. First, Defendants do not directly or indirectly inform Illinois users that they collect, capture, and store faceprints from users. Nor do Defendants require Illinois users to acknowledge their collection and storage of their biometric data, much less obtain a written release from them before collecting their faceprints. Instead, Defendants market their "Face Blur" tool as protecting "anonymity" and their thumbnail creator as simply a beneficial feature for YouTube video creators. Defendants never give any indication that use of these features would come at the cost of Illinois users' biometric privacy rights.

---

[25] *Id.*

80. Secondly, and compounding these problems and their violations of BIPA, YouTube's website does not have a written, publicly available policy identifying its biometrics retention schedule, nor guidelines for permanently destroying Illinois users' biometric identifiers when they are no longer needed.

81. The uploading, Defendants' capture, and Defendants' use of Plaintiff's and Class members' biometric identifiers, and Defendants' failure to post a publicly available retention schedule and guidelines for permanently destroying such biometric identifiers, along with their failure to comply with such, also took place in Illinois.

82. By and through these actions, Defendants not only disregarded their Illinois users' privacy rights, but they also violated their statutorily protected rights to control the collection, use, and storage of their sensitive biometric data.

## VII. Plaintiff's Experiences

83. Plaintiff Colombo has been a registered YouTube user since at least March 2020. Since then, Colombo has uploaded multiple videos to his YouTube account that include images of his face. Such videos were uploaded within the state of Illinois, collected by Defendants within the state of Illinois, and used by Defendants in the state of Illinois.

84. On each occasion, YouTube auto-generated thumbnail photographs from Colombo's video uploaded within the state of Illinois. On multiple separate occasions, YouTube auto-generated a thumbnail photograph from one of Colombo's uploaded videos containing his face. In generating these thumbnails, Defendants' tools necessarily produced information that can be used in identifying Colombo, which Defendants subsequently captured, used, and stored.

85. On one occasion while in Illinois, Colombo uploaded a video to YouTube that contained his face and scanned his face using the "Face Blur" tool.

86. Because Defendants failed to ***develop*** or implement a BIPA-compliant data collection policy, Defendants therefore failed to ***comply*** with any BIPA-compliant policy in their handling of Plaintiff's personally identifying information. As a result, Plaintiff was never informed of Defendants' personally identifying data collection, and Plaintiff never consented, agreed, or gave permission – written or otherwise – to Defendants to collect or store his biometric identifiers. Further, Plaintiff was never provided with, nor ever signed, a written release allowing Defendants to collect or store his biometric identifiers.

87. Worse still, Defendants never even informed Plaintiff by written notice or otherwise that he could prevent Defendants from collecting or storing his biometric identifiers.

88. Likewise, Plaintiff was never provided with an opportunity to prohibit or prevent Defendants from collecting or storing his biometric identifiers.

89. Nevertheless, when Plaintiff uploaded videos to his YouTube account within the state of Illinois, Defendants scanned the faces (including his) in the videos, located his face, and created or extracted a unique faceprint or "template" for him containing his biometric identifiers, including his facial geometry. Defendants subsequently stored Plaintiff's biometric identifiers.

90. Plaintiff has suffered cognizable harm and been aggrieved by Defendants' BIPA violations alleged herein.[26]

## CLASS ALLEGATIONS

91. **Class Definition**: Plaintiff brings this action pursuant to Rule 23 of the Federal Rules of Civil Procedure on behalf of himself and a Class of similarly situated individuals, defined as follows:

> All residents of the State of Illinois who, while located in Illinois, had their faceprints or face templates collected, captured, received, or otherwise obtained by Defendants through videos uploaded to YouTube within Illinois.

92. The following people are excluded from the Class: (a) any Judge or Magistrate presiding over this action and members of their families; (b) Defendants, Defendants' subsidiaries,

[26] *See Rosenbach v. Six Flags Ent. Corp.*, 2019 IL 123186, ¶ 40, 129 N.E.3d 1197, 1207 ("[A]n individual need not allege some actual injury or adverse effect, beyond violation of his or her rights under [BIPA], in order to qualify as an 'aggrieved' person and be entitled to seek liquidated damages and injunctive relief pursuant to [BIPA].").

parents, successors, predecessors, and any entity in which the Defendants or their parents have a controlling interest and its current or former employees, officers and directors; (c) persons who properly execute and file a timely request for exclusion from the Class; (d) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (e) Plaintiff's counsel and Defendants' counsel; and (f) the legal representatives, successors, and assigns of any such excluded persons.

93. **Numerosity**: The exact number of Class members is unknown to Plaintiff at this time, but it is clear that individual joinder is impracticable. Defendants have collected, captured, received, or otherwise obtained biometric identifiers from at least hundreds of thousands (and potentially even millions) of individuals who fall into the definition of the Class. Ultimately, the Class members will be easily identified through Defendants' records.

94. **Commonality and Predominance**: There are many questions of law and fact common to the claims of Plaintiff and the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include the following:

(a) whether Defendants collected, captured, received, or otherwise obtained Plaintiff's and Class members' biometric identifiers;

(b) whether Defendants properly informed Plaintiff and the Class that they collected, used, and stored their biometric identifiers;

(c) whether Defendants obtained a written release (as defined in 740 ILCS 14/10) from Plaintiff and the Class to collect, capture, or otherwise obtain their biometric identifiers;

(d) whether Defendants had and made available to the public, a written policy establishing a retention schedule and guidelines for permanently destroying biometric identifiers in compliance with BIPA; and

(e) whether Defendants' violations of BIPA were committed intentionally, recklessly, or negligently.

95. **Typicality**: Plaintiff's claims are typical of the claims of all other members of the Class. Plaintiff and Class members sustained substantially similar damages as a result of Defendants' uniform wrongful conduct, based upon the same transactions that were made uniformly with Plaintiff and the Class.

96. **Adequate Representation**: Plaintiff will fairly and adequately represent and protect the interests of the Class. Plaintiff has retained counsel with substantial experience in prosecuting complex class actions. Plaintiff and his counsel are committed to vigorously prosecuting this action on behalf of the members of the Class, and have the financial resources to do so. Neither Plaintiff nor his counsel have any interest adverse to those of the other members of the Class, and Defendants have no defenses unique to Plaintiff.

97. **Policies Generally Applicable to the Class**: Defendants have acted, or failed to act, on grounds generally applicable to Plaintiff and the other members of the Class, requiring the Court's imposition of uniform relief to ensure compatible conduct towards the Class.

98. **Superiority**: A class action is superior to all other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Class is impracticable. The damages suffered by the individual members of the Class are likely to have been small relative to the burden and expense of individual prosecution of the complex litigation necessitated by Defendants' wrongful conduct. Thus, it would be virtually impossible for the individual members of the Class to obtain effective relief from Defendants' misconduct. Even if members of the Class could sustain the cost of such individual litigation, it would not be preferable to a class action because individual litigation would increase the delay and expense to all parties due to the complex legal and factual controversies presented in this Complaint, and present a tremendous burden for the courts. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Economies of time, effort, and expense will be fostered and uniformity of decisions will be achieved.

## CAUSES OF ACTION

### COUNT I
### Violation of 740 ILCS 14/15(b)
### (On Behalf of Plaintiff and the Class)

99. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

100. BIPA makes it unlawful for any private entity to, among other things, "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier . . . unless it first: (1) informs the subject . . . in writing that a biometric identifier . . . is being collected or stored; (2) informs the subject . . . in writing of the specific purpose and length of term for which a biometric identifier . . . is being collected, stored, and used; ***and*** (3) receives a written release executed by the subject of the biometric identifier[.]" 740 ILCS 14/15(b) (emphasis added).

101. Defendants are Delaware corporations and thus each qualifies as a "private entity" under BIPA. *See* 740 ILCS 14/10.

102. As explained in detail above, Plaintiff's and Class members' faceprints or face geometry are "biometric identifiers" pursuant to 740 ILCS 14/10.

103. Defendants systematically and automatically collected, used, and stored Plaintiff's and Class members' biometric identifiers without first obtaining the specific written release required by 740 ILCS 14/15(b)(3). Defendants' collection and use of Plaintiff's and Class members' biometric identifiers took place within the state of Illinois.

104. As explained in detail above, Defendants did not properly inform Plaintiff or the Class in writing that their biometric identifiers were being collected and stored, nor did it inform them in writing of the specific purpose and length of term for which their biometric identifiers were being collected, stored, and used as required by 740 ILCS 14/15(b)(1)-(2).

105. By collecting, storing, and using Plaintiff's and Class members' biometric identifiers in the state of Illinois as described herein, Defendants violated Plaintiff's and Class members' rights to privacy in their biometric identifiers as set forth in BIPA, 740 ILCS 14/1, *et seq*.

106. On behalf of himself and the Class, Plaintiff seeks: (a) injunctive and equitable relief as is necessary to protect the interests of Plaintiff and the Class by requiring Defendants to comply with BIPA's requirements for the collection, storage, and use of biometric identifiers as described herein; (b) statutory damages of $5,000 per violation for the intentional and reckless violation of BIPA pursuant to 740 ILCS 14/20(2), or alternatively, statutory damages of $1,000 per violation pursuant to 740 ILCS 14/20(1) if the Court or jury finds that Defendants' violations were negligent; and (c) reasonable attorneys' fees, costs, and other litigation expenses pursuant to 740 ILCS 14/20(3).

**COUNT II**
**Violation of 740 ILCS 14/15(a)**
**(On Behalf of Plaintiff and the Class)**

107. Plaintiff incorporates the foregoing allegations in paragraphs 1 through 98 as if fully set forth herein.

108. Section 15(a) of BIPA requires that any "private entity in possession of biometric identifiers . . . must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers . . . when the initial purpose for collecting or obtaining such identifiers . . . has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first." 740 ILCS 14/15(a).

109. For all YouTube users, Defendants do not publicly provide a retention schedule or guidelines for permanently destroying users' biometric identifiers as specified by BIPA. *See* 740 ILCS 14/15(a). Indeed, because Defendants had no retention schedule policy and made no such policy available to the public, Defendants failed to comply with a BIPA-compliant policy in their handling of Plaintiff's and Class members' personally identifying data.

110. Accordingly, on behalf of himself and the Class, Plaintiff seeks: (a) injunctive and equitable relief as is necessary to protect the interests of Plaintiff and the Class by requiring Defendants to establish and make publicly available a retention schedule or guidelines for permanently destroying its users' biometric identifiers as specified by BIPA; (b) statutory damages of $5,000 per violation for the intentional and reckless violation of BIPA pursuant to 740 ILCS 14/20(2), or alternatively, statutory damages of $1,000 per violation pursuant to 740 ILCS 14/20(1)

if the Court or jury finds that Defendants' violations were negligent; and (c) reasonable attorneys' fees, costs, and other litigation expenses pursuant to 740 ILCS 14/20(3).

**PRAYER FOR RELIEF**

WHEREFORE, Plaintiff, on behalf of himself and the Class, respectfully requests that this Court enter an Order:

A. Certifying this case as a class action on behalf of the Class defined above, appointing Plaintiff as representative of the Class, and appointing his counsel as Class Counsel;

B. Declaring that Defendants' actions, as set out above, violate BIPA, 740 ILCS 14/1, *et seq*.;

C. Awarding statutory damages of $5,000 per violation for the intentional and reckless violation of BIPA pursuant to 740 ILCS 14/20(2), or alternatively, statutory damages of $1,000 per violation pursuant to 740 ILCS 14/20(1) if the Court or jury finds that Defendants' violations were negligent;

D. Awarding injunctive and other equitable relief as is necessary to protect the interests of the Class, including, among other things, an Order requiring Defendants to collect, store, and use biometric identifiers in compliance with BIPA;

E. Awarding Plaintiff and the Class their reasonable litigation expenses and attorneys' fees;

F. Awarding Plaintiff and the Class pre- and post-judgment interest, to the extent allowable; and

G. Awarding such other and further relief as equity and justice may require.

**JURY TRIAL**

Plaintiff demands a trial by jury for all issues so triable.

DATED: June 13, 2023

ROBBINS GELLER RUDMAN
& DOWD LLP
STUART A. DAVIDSON (*pro hac vice*)
ALEXANDER C. COHEN (*pro hac vice*)

*s/ Stuart A. Davidson*
Stuart A. Davidson

225 NE Mizner Boulevard, Suite 720
Boca Raton, FL 33432
Telephone: 561/750-3000
561/750-3364 (fax)
sdavidson@rgrdlaw.com
acohen@rgrdlaw.com

ROBBINS GELLER RUDMAN
& DOWD LLP
AELISH M. BAIG
JACOB G. GELMAN
Post Montgomery Center
One Montgomery Street, Suite 1800
San Francisco, CA 94104
Telephone: 415/288-4545
415/288-4534 (fax)
aelishb@rgrdlaw.com
jgelman@rgrdlaw.com

MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN, PLLC
GARY M. KLINGER
221 West Monroe Street, Suite 2100
Chicago, IL 60606
Telephone: 866/252-0878
gklinger@milberg.com

MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN, PLLC
JONATHAN B. COHEN
800 South Gay Street, Suite 1100
Knoxville, TN 37929
Telephone: 865/247-0080
jcohen@milberg.com

MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN, PLLC
NICK SUCIU, III
6905 Telegraph Road, Suite 115
Bloomfield Hills, MI 48301
Telephone: 313/303-3472
nsuciu@milberg.com

Attorneys for Plaintiff and the Class

CERTIFICATE OF SERVICE

I hereby certify under penalty of perjury that on June 13, 2023, I authorized the electronic filing of the foregoing with the Clerk of the Court using the CM/ECF system which will send notification of such filing to the e-mail addresses on the attached Electronic Mail Notice List, and I hereby certify that I caused the mailing of the foregoing via the United States Postal Service to the non-CM/ECF participants indicated on the attached Manual Notice List.

*s/ Stuart A. Davidson*
STUART A. DAVIDSON